NetSight®

End to end application visibility and control

Unified LAN/WLAN management system simplifies tools and automates management tasks across the entire infrastructure

Easy policy enforcement, network-wide, ensures the availability of network resources for today's bandwidth intensive applications

Highly automated capabilities avoid time-consuming manual tasks for consistency and increased efficiency

Specialized identity and access management for visibility and control of users' devices

Anytime, anywhere management from popular mobile devices for the fastest response times

Product Overview

Enterasys NetSight's rich set of integrated management capabilities provides centralized visibility and highly efficient anytime, anywhere control of enterprise wired and wireless network resources. NetSight is distinguished by web-based OneView, the unified control interface. Graphical and exceptionally easy-to-use, OneView simplifies troubleshooting, help desk support tasks, problem solving and reporting. It's Identity and Access interface provides specialized visibility and control for the exploding number of managed and unmanaged devices connecting to today's networks.

Capability	Benefits
NetSight with Wireless Management Graphically displays aggregated wired and wireless network information for centralized and simplified management of all infrastructure components as a single system	• Combines WLAN/LAN management for greater IT operational efficiency • Facilitates communication and alignment between IT and line of business • Adds value to existing management platforms • Reduces total cost of ownership
Policy Management Automates the definition and enforcement of network-wide policy rules controlling QoS, priority, bandwidth, and security	• Fully aligns the network infrastructure with business objectives • Simplifies policy lifecycle management easing IT burden • Reduces troubleshooting time • Minimizes risk of disruptions
Identity and Access Specialized OneView interface provides easy-to-use, exceptionally detailed information about connected end systems	• Enables efficient control in the BYOD environment • Visibility and policy enforcement end-to-end • Monitors and manages risk from unmanaged devices • Ensures network availability and performance
Automated Security Management Integrates with Enterasys IPS, NAC, SIEM, and other third party security appliances to respond automatically and remediate threats in real-time	• Protects corporate data and ensures network availability • Ensures response actions are policy-based and executed consistently • Reduces IT staff burden and costs
Network Access Control (NAC) Management Manages the Mobile IAM and NAC solutions providing granular control over users and applications, and featuring a high-level dash-board view of the complete security posture	• Ensures that only the right users have access to the right information from the right place and time • Maintains guest/contractor and user productivity • Simplifies end-system compliance monitoring and reporting • Delivers quick time to value
Inventory Management Automates management of device configurations and provides tools to capture, modify, load, and verify configurations	• Provides network control and better efficiency • Streamlines IT operations and enhances staff productivity • Enables audit efficiency and cost savings
OneView Unified web-based interface and fine-grained interactive search for network analysis, problem solving, help desk visibility and reporting	• State-of-the-art graphics reporting and topology displays enable efficiency and more effective communications • Simplifies troubleshooting, help desk support tasks, problem solving across wireless and wired networks • Streamlines wireless management
Mobile Management Optimizes network management and help desk troubleshooting with anywhere, anytime access to critical information using popular mobile devices	• Prevents loss of user productivity • Most responsive network management

Benefits

Business Alignment

- Transform complex network data into business-centric, actionable information
- Centralize and simplify the definition, management, and enforcement of policies such as guest access or personal devices
- Easily integrate with business apps with Software Defined Networking

Operational Efficiency

- Reduce IT administrative effort with the automation of routine tasks and web-based dashboard
- Streamline management with the integration of wired and wireless networks
- Easily enforce policies network-wide for QoS, bandwidth, etc.
- Troubleshoot with the convenience of a smart phone or tablet
- Integrate with enterprise management platforms

Security

- Protect corporate data with centralized monitoring, control, and real-time response
- Enhance existing investments in network security
- Preserve LAN/WLAN network integrity with unified policies

Service and Support

- Industry-leading first call resolution rates and customer satisfaction rates
- Personalized services, including site surveys, network design, installation and training

There is nothing more important than our customers

NetSight is distinctive for granularity that reaches beyond ports, VLANs and SSIDs down to individual users, applications, and protocols. NetSight increases efficiency, enabling IT staff to avoid time-consuming manual device-by-device configuration tasks. NetSight fills the functionality gap between traditional element managers that offer limited vendor-specific device control, and expensive, complex enterprise management applications. NetSight is a key component of OneFabric™ Control Center, Enterasys' predictive network management solution for end to end application delivery.

NetSight, with wireless management, is the foundation for centrally monitoring and managing all the components in the infrastructure. NetSight enables the network infrastructure to be viewed as a unified whole rather than as a collection of disparate individual components. It transforms complex network data into graphical, business-centric information making the network less complicated and better aligned with business requirements.

With its distributed client/server architecture, NetSight is exceptionally convenient to use. A user with appropriate security credentials anywhere on the network can access a launch page and log into any of the NetSight capabilities. NetSight simplifies routine and one-time tasks such as reconfiguring switches and access points, monitoring network performance, and isolating faults. It takes advantage of advanced functionality in Enterasys switching, routing, and wireless products including topology maps, FlexViews (graphical depictions of a broad range of network parameters), VLAN management, device discovery, and event logging. Enterasys NetSight supports management for IPv6 devices.

OneView Interface

Enterasys NetSight unifies all the capabilities under one web-based control interface. With OneView, critical network information is accessible and easy to use. This powerful tool enables both managers and technical staff to be more efficient in their monitoring, reporting, analysis, troubleshooting and problem solving tasks.

Highlights among the OneView capabilities include: wired/wireless dashboards, detailed identity and access information, reports, interactive topology maps, web-based FlexViews, device views and alarm and event management for the entire infrastructure. NetFlow diagnostics are incorporated into OneView enabling diagnosis of network issues and performance through real-time NetFlow analysis.

The OneView wireless dashboard streamlines network monitoring with consolidated status of all the devices and drill down ability for more details. State-of-the-art reporting provides historical and real-time data for high level network summary information and/or details. The reports and other views are interactive allowing users to choose the specific variables they need when analyzing data. Web-based FlexViews enable real-time diagnostics.

OneView's identity and access interface provides a dashboard summary of all connected systems with interactive charts and graphs for further details. Additional dashboards show information about the systems and appliances, and the health status of connected end systems. A unique end system view contains all the available details about connected systems solving a range of IT issues from troubleshooting user access to quickly identifying types devices (i.e.Windows, MAC, Android, IOS) and how they authenticated to the network.

OneView's search functionality is a powerful diagnostic tool. End systems are searchable by port, MAC address and IP or IP/Port. The results page provides an interactive topology map consolidating all the data sources available for that location such as performance data, NetFlow data and network access control data. Troubleshooting is simple and efficient with all the data in one graphical and easy to use page.

Wireless Management

Wireless management is integrated into NetSight providing a single launch point for wired/wireless management and common management functionality. NetSight's integrated wired/wireless management, streamlines IT effort and lowers costs. Configuration changes are specified and deployed in minutes rather than hours. A single administrator can manage significantly more users and devices by utilizing the inherent automation features in NetSight.

The OneView interface enables highly efficient monitoring, analysis and troubleshooting. For wireless management, OneView features coverage maps, location maps, wireless summary dashboards, reports, topology display for end-system troubleshooting and wireless client statistics analysis and reporting. The OneView wireless management information available with mobile management makes control easy and responsive with the convenience of a smart phone or tablet.

Policy Management

NetSight policy management centralizes all the policies for users, applications, protocols, VLANs, ports, and data flows. It automates the definition, distribution, and enforcement of policy rules across the entire network. With an intuitive user interface, administrators can define policies once and then automatically enforce them on Enterasys policy-enabled infrastructure devices.

Unified wired/wireless policy management consolidates user access to protect IT services. Policy management defines global user policies, dynamically updates and continuously enforces policy across wired and wireless environments. Packets are inspected and filtered at the AP and admitted or blocked based on the user's policy. Policy also controls topology management, traffic flows and unlimited Class of Service for wireless controllers.

Policy is role-based, significantly streamlining policy administration. Individual users with similar behavior profiles, such as sales managers, executives, or guest users are grouped into a far smaller number of roles. Applying roles makes it far easier to align the network infrastructure with the business and control guest users, enforce regulatory mandates, and enforce acceptable use rules.

Policy management includes a unique tool for delegating limited administration controls to non-technical line of business users. From a secure web-based console, a delegated user such as a line of business manager, receptionist, or classroom instructor can easily select a policy to implement. Policies are enabled or disabled with a simple mouse click and changes are instantly acknowledged on the console.

Network Access Control Management

Network Access Control (NAC) management combines with Enterasys NAC appliances or virtual appliances for a complete network access control solution, ensuring that only the right users have the right access to the right information from the right place at the right time.

NAC management software provides secure, policy-based NAC management. From one, centralized location IT staff can configure and control the NAC solution, simplifying deployment and on-going administration. The Enterasys NAC IP-to-ID Mapping capability binds together the username, IP address and MAC address, and physical port of each endpoint. NetSight reports this important information for audit or forensics analysis.

NAC management provides additional value through its integration with other NetSight capabilities and Enterasys security products. For example, NAC management with policy management enable "one click" enforcement of role-based policies. IP-to-ID Mapping is also used by ASM for location-independent distributed intrusion prevention and by Enterasys Security Information & Event Manager (SIEM) to pinpoint the source of the threat.

Inventory Management

NetSight inventory management efficiently documents and updates the details of the ever-changing network. It simplifies the deployment and management of Enterasys devices and supports basic configuration and firmware device management functions for popular third party devices. IT staff can easily perform a broad list of tasks including device administration on configuration files, schedule firmware updates, archive configuration data, or restore one or multiple devices to a known good state. Script-based configuration allows custom configuration scripts to be pushed to a set of devices. NetSight identifies unused ports and chassis slots and tracks moves, adds, and changes for Field Replaceable Units.

Inventory management also tracks configuration changes for Enterasys devices made by NetSight, third-party management applications, or the command line interface.

Automated Security Management

Automated Security Management is a unique threat response solution that translates security intelligence into security enforcement. It interoperates with the Enterasys Intrusion Prevention System (IPS) and third-party network security appliances to automate responses to security incidents, remediating threats in real-time. It ensures that corporate data is protected, secure, and available.

ASM executes policy-based rules, and when triggered, maps IP addresses to ports and takes assigned actions. The range of possible response actions is broad and configurable, including quarantining the user, disconnecting a wired or wireless client, or rate-limiting the traffic flow. Taking the action does not disrupt other users.

Combined with policy management functions and IPS, ASM provides sophisticated identification and management of threats and vulnerabilities. For example, when notified by the IPS, ASM can determine the exact source location of a threat, determine a response based on the security policy, and trigger the configured action on the network switch, access point or wireless controller.

Mobile Management

NetSight mobile management extends OneView optimizing network management and help desk troubleshooting with anywhere, anytime access to critical information using popular mobile devices such as iPad®, iPhone® and Android™ devices. Capabilities include: Network Access Control (NAC) end-system view, system location and tracking, wireless dashboards; detailed views of controllers and APs; event logs, and wireless client search.

OneFabric Connect/SDN

The Enterasys OneFabric Connect API provides a simple, open, programmable and centrally managed way to implement Software Defined Networking (SDN) for any network. With OneFabric Connect, business aplications can be directly controlled from the OneFabric Control Center Advanced managed via NetSight. The result is a complete SDN solution. More information is available in the OneFabric Connect API Datasheet.

NetSight Features

IPv6
Enterasys NetSight supports IPv6 management for IPv6 capable devices.

Device Discovery
The discovery process locates network attached devices, stores attributes for these devices, and reports device status. Devices may be discovered automatically by specifying an IP address range or via both standard and multiple vendors' proprietary discovery protocols. Devices may also be added manually or imported into the NetSight database using a device list file.

Network Topology Maps
A topology map is an automatically generated visual representation of network connectivity. Topology maps, encompassing integrated wired and wireless networks, provide network administrators with in-depth graphical views of device groupings, device links, VLANs, and Spanning Tree status. Color codes are used to indicate device status and SNMP/ SNMPv3 or information traps are easily generated.

FlexViews and Graphing
Incorporating both wired and wireless systems, FlexViews are Console tools that allow network support staff to view a broad range of network configuration parameters in graphical format—including tables, bar graphs, line graphs, and pie charts. FlexView data is searchable and sortable. For example, an administrator can use a FlexView to quickly determine the top instances of ports with sustained load over 30% across all networked devices.

Console ships with pre-defined FlexViews that depict status and configuration information for the entire network. An administrator can easily modify and apply filters to these pre-defined FlexViews, or create additional ones. FlexView data may also be exported in CSV, XML, and HTML formats.

RealCapture
RealCapture allows the on-demand, real time collection of over-the-air traffic for troubleshooting and problem resolution. It gives IT administrators visibility into the RF environment for quicker problem resolution.

Basic Policy Management
Basic Policy Management allows users to view and configure port default policy for network attached devices. Use Basic Policy Management to view information about each port login session, including authentication type and authenticated user role.

Compass
Compass is an endpoint and user search tool that allows the user to quickly locate information pertaining to an individual network user or group of users across the integrated wired and wireless network. It provides searches by user name, switch authentication, physical location, MAC address, IP address, IP Subnet, and other parameters.

VLAN Tools
Console includes a set of VLAN management tools to simplify the system-wide deployment of VLAN configuration and monitoring capabilities. Using these tools a user can easily create VLAN configuration parameters which may be deployed automatically to multiple devices or to groups of ports.

MIB Browser Tools
Console's Management Information Base (MIB) Browser allows the user to examine the SNMP MIB variables of network attached devices and set the values of writable MIB objects.

Alarms and Events
NetSight provides advanced alarm management significantly reducing problem response time. Any event can be configured to create an alarm along with a color-coded severity scheme. Alarms may be configured based on statistical thresholds. Alarm actions such as emails or other notifications are completely configurable. Alarms are highly visible including at-a-glance alarm status integrated with existing displays and visual indicators in device status. Alarm information may be archived, exported, filtered or searched. Alarm clearing can be manual or automatic.

Ease of Installation
All NetSight client-server applications are installed in a single step and the license key automatically determines which features are enabled. Product upgrades to add additional functionality are fast and straightforward. The Java®-based NetSight client application is automatically installed and launched by clicking on a URL and is automatically upgraded if not at the correct revision level. This ensures that the server and client are always in sync, and all installation and upgrades only need to be performed on the server. The NetSight client supports single sign-on so users are prompted just once for their authentication credentials across any of the NetSight capabilities. Permission consistency also limits user access to only authorized MIB information.

Database Backups
Administrators can schedule backups of the NetSight database for easier recovery.

Failover
NetSight may be implemented in failover mode when it is deployed as a virtual machine. Leveraging VMware ESC and vCenter, an automatic failover based on hardware failure is provided if contact to the NetSight server is lost.

Deployment Flexibility

NetSight is typically downloaded and installed on enterprise server machines. It is also available as an appliance or virtual appliance for enterprises that seek the benefits of these other deployment alternatives.

NetSight Appliance – server with all capabilities pre-installed (activated via license keys) for enterprises that prefer the easy deployment of an appliance.

NetSight Virtual Appliance – virtual appliance with capabilities pre-installed (activated via license keys) for enterprises who wish to further leverage their virtualized environments. It provides all the benefits of the management suite with the advantages of a virtual environment – simple installation and cost savings from the use of existing hardware.

System Requirements

NetSight Server and Client OS Requirements
These are the operating system requirements for both the NetSight Server and remote NetSight client machines.

Windows (qualified on the English version of the operating systems)
Windows Server® 2003 w/ Service Pack 2 (64-bit & 32-bit)
Windows XP® w/ Service Pack 2 or 3 (32-bit only)
Windows Server® 2008 Enterprise (64-bit & 32-bit)
Windows® 7 (64-bit & 32-bit)
Windows® 8 (64-bit & 32-bit)

Linux
Red Hat Enterprise Linux WS and ES v5and v6 (64-bit & 32-bit)
SuSE Linux versions 10 and 11 (64-bit & 32-bit)
Ubuntu 11.10 Desktop version (32-bit for remote NetSight client only)
Ubuntu 11.10 and 12.04 (64-bit)

Mac OS X® 64-bit (remote NetSight client only)
Leopard®, Snow Leopard®, Lion® or Mountain Lion®

VMware® (64-bit NetSight Virtual Appliance)
VMware ESXi™ 4.0, 4.1, 5.0 or 5.1 server

NetSight Server and Client Hardware Requirements
These are the hardware requirements for the NetSight Server and NetSight client machines:

NetSight Server
Minimum - Dual-Core 2.4 GHz Processor, 2 GB RAM,
5 GB Free Disk Space

Medium - Quad-Core 2.66 GHz Processor, 4 GB RAM,
10 GB Free Disk Space

Large - Dual Quad-Core Intel® Xeon CPU E5530 2.4 GHz Processors (running Red Hat Enterprise Linux ES), 6 GB RAM, 20 GB Free Disk Space

NetSight Client
Recommended - Dual-Core 2.4 GHz Processor, 2 GB RAM
Free Disk Space - 100 MB
(User's home directory requires 50 MB for file storage)
Supported Web Browsers:
- Internet Explorer version 8 and 9
- Mozilla Firefox 11 and 12
- Google Chrome 19.x

Java Runtime Environment (JRE) 6 or 7 (also referred to as 1.6 or 1.7)

NetSight OneView
OneView supports reporting on about 2,500 devices/interfaces in a typical enterprise network which stores: raw data for 7 days with a 15 minute polling interval, hourly rollups for 8 weeks, and daily rollups for 6 months. More information on tuning the deployment is available in the OneView Users Guide.

NetSight Appliance
For NetSight Appliance specifications see the Enterasys NetSight Appliance Installation Guide.

NetSight Virtual Appliance
A virtual appliance is a software image that runs on a virtual machine. The NetSight virtual appliance is packaged in the .OVA file format defined by VMware and must be deployed on a VMware ESX™ 4.0, 4.1 or 5.0 server or ESXi™ 4.0, 4.1 or 5.0 server with a vSphere™ 4.0, 4.1 or 5.0 client.

The NetSight virtual appliance uses the following resources from the server it is installed on:

- NetSight virtual appliance - configured with 8 GB of memory, four CPUs, two network adapters, and 60 GB of thick-provisioned hard drive space.

Ordering Information

Enterasys NetSight provides cost-efficient choices enabling enterprises to address their priorities, optimize their budget use and demonstrate quick time-to-value. NetSight models range from a cost-efficient entry solution to full functionality for device intensive enterprises. Flexible upgrade options support deployment growth.

The three NetSight models are:

NMS-BASE-XX which includes basic wired/wireless management features as well as inventory management, policy management and OneView Basic (device management, alarm management and administration). 3 remote clients are included in addition to unrestricted OneView connections.

NMS-XX which includes basic wired/wireless management features as well as inventory management, policy management, NAC management, automated security management, mobile management, and the full OneView interface. 25 remote clients are included in addition to unrestricted OneView connections.

NMS-ADV-XX which includes basic wired/wireless management features as well as inventory management, policy management, NAC management, automated security management, mobile management, and the full OneView interface. In addition, NetSight Advanced includes advanced wireless management, the OneFabric Connect API, ability to install on a primary server, redundant server and lab server, and virtual NAC appliances for full NAC deployment flexibility (require end-system licenses). 25 remote clients are included in addition to unrestricted OneView connections.

NetSight sizing chart

# Managed Devices	# Aps	Model Numbers		
5	50	NMS-ADV-5	NMS-5	
10	100	NMS-ADV-10	NMS-10	NMS-BASE-10
25	250	NMS-ADV-25	NMS-25	NMS-BASE-25
50	500	NMS-ADV-50	NMS-50	NMS-BASE-50
100	1,000	NMS-ADV-100	NMS-100	NMS-BASE-100
250	2,500	NMS-ADV-250	NMS-250	NMS-BASE-250
500	5,000	NMS-ADV-500	NMS-500	NMS-BASE-500
Unrestricted	Unrestricted	NMS-ADV-U	NMS-U	NMS-BASE-U

NetSight Appliance

SNS-NSS-A	Rack mountable server with all capabilities pre-installed. Purchased application (licensed separately) is activated via license key

Warranty

As a customer-centric company, Enterasys is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

The NetSight Appliance comes with a one year warranty against manufacturing defects. Software warranties are ninety (90) days, and cover defects in media only. For full warranty terms and conditions please go to: www.enterasys.com/support/warranty.aspx.

Service and Support

Enterasys Networks provides comprehensive service offerings that range from Professional Services to design deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Enterasys account executive for more information about Enterasys Service and Support.

Additional Information

For additional technical information on NetSight please go to: http://www.enterasys.com/products/visibility-control/index.aspx.

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com

Thought Leadership
Patented Innovation

© 2012 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit http://www.enterasys.com/company/trademarks.aspx for trademark information.

enterasys® Secure Networks™

Delivering on our promises. On-time. On-budget.